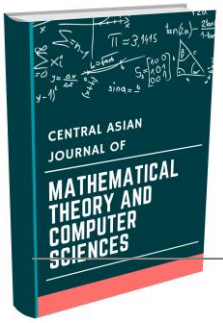

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 1 | Jan 2023 ISSN: 2660-5309

ON THE THEORY OF RELIABILITY OF THE SYSTEM OF PROTECTION AGAINST UNAUTHORIZED ACCESS TO INFORMATION

Ibrokhimali Normatov, Bobur Ergashev, Murodulla Boboqulov

National university of Uzbekistan named after Mirzo Ulugbek

Abstract

The development and increase in efficiency of computer technology leads to the need to work in conditions of increased noise level, which can be accompanied by unbalanced heat output, low signal level and, as a result, failures and errors in the obtained results. This research paper investigates the unauthorized leakage of information. And the essence of the problem is revealed with the help of graphs, it is transferred from the graphs to the matrix view. The research can be applied to information security assessment issues.

ARTICLEINFO

Article history:
Received 6 Nov 2022
Revised form 5 Dec 2022
Accepted 24 Jan 2023

Keywords: *unauthorized access, information security, theory graph, theory of reliability, semi-Markov process, probability matrix.*

Introduction

Information technologies are information management and processing technologies. Computer technology is usually understood under this term. In the field of information technologies[1-6], work is carried out on operations such as collection, storage, protection, processing, transmission of various information through ECM and computer networks[7-12]. When applied to hard disks, it looks like this: with the existing recording density, it is no longer possible to read the signal from the surface of the disk - the level of noise and distortion is too high. Instead of directly changing the signal, it is used to compare it with a set of samples, and based on the maximum similarity (probability), it is correct to accept one or another machine word a conclusion is drawn. All this leads to a revival of interest in assessing the impact of computer equipment failures and malfunctions on the tasks they solve, including the tasks of protecting information[13-18] from unauthorized access. Currently, domestic developers offer technical means of information protection certified by the International Technical Commission of the world against unauthorized access to automated systems[19-23], such as Secret Net, Dallas Lock, etc. Thus, in such products, protective functions are performed using technical means located on a completely separate board. This option maximally separates the technical means of processing protected data and the technical means that perform the functions of protection against unauthorized access to information. At the same time, the data protection[24-27] program is stored in the memory of the "Harvard" architecture microprocessor, the technology of writing the program to "long-term memory" separates its virus infection, RAM and program memory. In Dallas Lock, the main functions of Secret Net products, software and data protection against unauthorized access are "trusted" to the usual elements located on the motherboard of the personal computer,

as well as to the external storage medium that stores the data protection software. from unauthorized access. An analysis of options for information protection systems against unauthorized access is also presented.

The technique [3] makes it possible to evaluate these principles of implementation in terms of efficiency indicators - the security of information from malicious study. Of particular interest is the assessment:

- the influence of the reliability of technical means of protecting information from UA on the functions of protecting information;
- known options for constructing a system for protecting information from unauthorized access from the point of view of reliability theory;
- the influence of the organization of monitoring the performance of technical means on the functions of protecting information from unauthorized access;
- formation of requirements for the components of the system for monitoring the performance of technical means of protecting information from unauthorized access.

The listed tasks can be solved if there is an appropriate mathematical apparatus and evaluation methods. This article proposes a mathematical apparatus, as well as a methodology that makes it possible to assess the impact of the reliability of technical information security facilities from unauthorized access on information security functions and make a decision on this range of tasks. An example is considered that makes it possible to compare information protection systems from UA of the ACKORD and Secret Net types, as well as Dallas Lock, in terms of the effectiveness of the reliability of technical means that implement the functions of protecting information from UA.

Mathematical model of functioning of the system of protection against unauthorized access to information based on the theory of reliability

Systems for protecting information from unauthorized access implement the following tasks (functions), the implementation of which is mandatory to achieve high levels of AS security [2].

T1. Perform identification and authentication with guaranteed protection against destructive software impacts.

T2. Control of the integrity of the AS hardware and software environment.

T3. Real data reading control.

T4. Access control to all file system objects.

T5. Task launch control.

T6. Maintaining an isolated software environment.

The rate of launching the tasks of this set is determined by the rate of launching the user's tasks.

Undetected failures or failures of individual elements of the technical Information Protection System from unauthorized access lead to a decrease in the reliability of the functioning of the entire technical means of protecting information from unauthorized access. The exceptional importance of solving the above tasks involves the creation in the technical system of protecting information from unauthorized access of a system for monitoring their performance.

In the general case, the process of functioning of a system protected from unauthorized access can be considered as an interaction process:

- information to be protected;
- functions of protecting information from unauthorized access (list T1 - T6);
- failures and failures of technical Information Security System;
- systems for monitoring the operability of these technical means;
- systems for restoring the operability of technical means.

A careful consideration of their interaction allows us to identify a process characterized by a finite set of possible states that uniquely determine the state of the system under study at each moment of time

$$S = \{S_1, S_2, \ldots\ldots, S_r\}. \quad (1)$$

At the same time, the functioning of the system under study is a process of transitions from one state to another (process steps).

The probability that at the next step the system will pass from state Si to state Sj generally depends on the initial state of the system and on all intermediate states up to the current one. At present, chains with the Markov property (processes of transition from the past to the future through the present) have been studied in the most detail. In this case, the probability of transition at the next step from the state Si to the state Sj depends only on the state Si, in which the system under study found itself after the previous step. It is natural to assume that:

- the probability of a simultaneous change in the states of two or more elements (for example, an event occurred associated with the failure or failure of an element of the Information Security System from unauthorized access and the end of the implementation of some function of protecting information from unauthorized access, etc.) is negligible;
- probabilities of transitions from one state to another do not depend on time;
- for an infinitely small period of time, it is impossible to transition to some neighboring state and return from it.

The overwhelming predominance of processes of a random nature in our case allows us to consider this process as an ergodic semi-Markov process [6] with a transition probability matrix of an ergodic chain.

$$P = \begin{matrix} P_{11} & P_{12} & \ldots & P_{1r} \\ P_{21} & P_{22} & \ldots & P_{2r} \\ \ldots & \ldots & \ldots & \ldots \\ P_{r1} & P_{r2} & \ldots & P_{rr} \end{matrix} \quad (2)$$

with $S = \{S1, S2, .., Sr\}$ −the set of return states of the semi-Markov process and the average residence time in each of the return states $m_i, S_i \in S$.

Obtaining a mathematical expression for assessing the reliability of the implementation of information protection functions of the system under research

The construction of a mathematical model for evaluating the system under study in terms of efficiency - the reliability of the implementation of the information security function - is based on the order of its construction, considered in detail in [6].

Errors in the implementation of the information protection functions from UA are the result of undetected failures and failures of technical means that implement the function of protecting information from UA (it is assumed that the program for protecting information from UA has no errors). Since undetected failures can lead to incomplete implementation of information protection functions from UA (erroneous results of process control from UA to protected information), we will consider their effect similar to the effect of failures.

Therefore, when calculating the reliability of the implementation of information protection functions against unauthorized access, undetected failures and failures do not differ and are called failures.

The organization of the interaction of information to be protected, the functions of protecting information from UA (list T1 - T6), failures and failures of technical means of protecting information, the system for monitoring the performance of technical means of protecting against UA, the system for restoring the operability of technical means in the general case can be set in the following form. Let the elementary flow of tasks with the parameter β arrive at the input of the protected system. The means of control of the first type with probability P1 detect failures during the implementation of the information protection function instantly. In addition, at the end of the implementation of the protection function, a failure is detected with a probability - P2 based on the results of program-logical control. The duration of the implementation of the information protection function on an operable and inoperable technical means of protection is, in the general case, a random value distributed according to an exponential law with the parameter γ. When the technical means of protecting information from unauthorized access is not busy implementing the information protection function, a test problem is solved. The test task implementation time is distributed according to the exponential law with the parameter θ. The arrival of a request for the implementation of the function of protecting information from UA automatically terminates the decision of the latter. When solving a test problem, hardware failures are detected instantly with a probability of P3, and with a probability of P4 - after the completion of a fully implemented test check. It is assumed that all values are $0 \leq P_i \leq 1$. In all cases of detection of a failure (calculation errors), technical means of protecting information from unauthorized access are sent for restoration, after which the solution of the problem is repeated on request or work continues according to the test program. The flows of failures and restorations are assumed to be the simplest ones with parameters λ and μ, respectively. Thus, the impact of monitoring the performance of a technical means of protecting information from UA is reduced to the fact that its failure can be detected before the implementation of the function of protecting information from UA therefore, the readiness of the module to perform the function of protecting information from UA increases and, accordingly, the reliability of the implementation of the function of protecting information from UA increases. The states of the technical means of protecting information from unauthorized access differ depending on whether a request has been received to implement the function of protecting information from unauthorized access, or whether a failure has occurred in the module. The set of states of the technical means of protecting information from unauthorized access is specified as follows:

S1 - there is no request for the implementation of the protection function against unauthorized access (hereinafter referred to as requests), the technical means of protecting information from unauthorized access is operational and solves the test problem;

S2 - no requests, the technical means of protecting information from UA has failed and is being restored;

S3 - no requests, the technical means of protecting information from unauthorized access has failed, the test problem is being solved, but the failure has not been detected;

S4 - the received request is processed on a workable technical means of protecting information from unauthorized access;

S5 - the received request for the implementation of the function of protecting information from UA on the failed technical means of protecting information from UA is being processed;

S6 - there is a request, but the failed technical means of protecting information from unauthorized access is being restored.

The transition graph of the described interaction model is shown in Figure 1

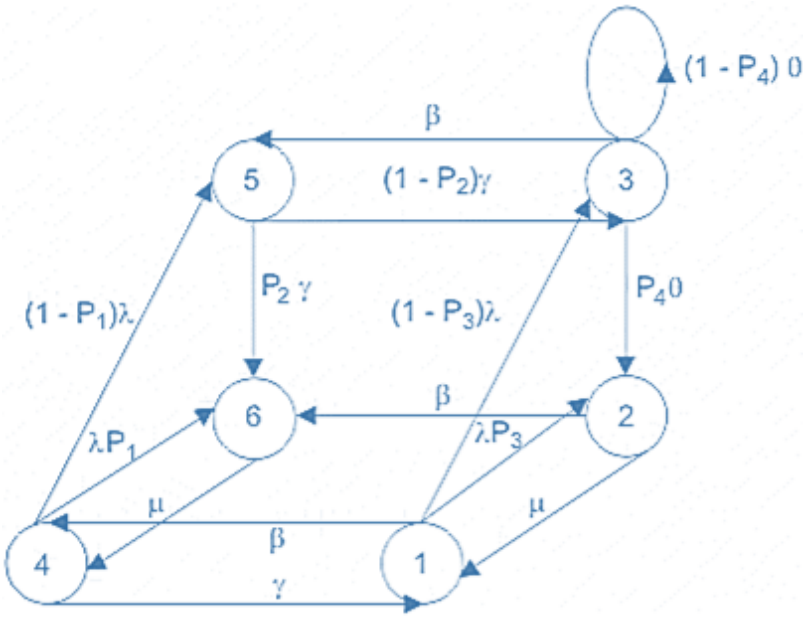

Figure 1. Graph of transitions of the studied technical means of protecting information from unauthorized access

This transition graph corresponds to the matrix P of transition probabilities of the nested Markov chain and the vector $||m_i||$ of average residence times of the semi-Markov process in each state $S_i \in S$ ($i \in [1,6]$), defined as:

$$P = \begin{matrix} 0 & \frac{p_3\lambda}{\beta+\lambda} & \frac{(1-p_3)\lambda}{\beta+\lambda} & \frac{\beta}{\beta+\lambda} & 0 & 0 \\ \frac{\mu}{\beta+\mu} & 0 & 0 & 0 & 0 & \frac{\beta}{\beta+\mu} \\ 0 & \frac{p_4\theta}{\beta+\theta} & \frac{(1-p_4)\theta}{\beta+\theta} & 0 & \frac{\beta}{\beta+\theta} & 0 \\ \frac{\gamma}{\lambda+\gamma} & 0 & 0 & 0 & \frac{(1-p_1)\lambda}{\lambda+\gamma} & \frac{p_1\lambda}{\lambda+\gamma} \\ 0 & 0 & 1-p_2 & 0 & 0 & p_2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}$$

$$\|m_i\| = \frac{1}{\beta+\lambda} \quad \frac{1}{\beta+\mu} \quad \frac{1}{\beta+\theta} \quad \frac{1}{\lambda+\gamma} \quad \frac{1}{\gamma} \quad \frac{1}{\mu}.$$

Derivation of a mathematical expression to estimate the average time of safe operation of the system under research

The assessment of the reliability of the implementation of the functions of protecting information from unauthorized access is informative and makes it possible to compare various options for constructing a system for protecting against unauthorized access. When comparing options for building an information protection system from unauthorized access, estimates may differ slightly, but the weight of this insignificance can be significant. As a result, it is advisable to compare them in terms of efficiency - the average time of safe operation (the average time between incorrect conclusions about UA).

The analysis shows that the transition graph in Figure 1 does not allow determining the time interval between adjacent incorrect conclusions about UA (the time interval for the safe operation of a technical means of protecting information about UA). Let us introduce an absorbing state S7 - the state of an undetected failure of a technical means of protecting information from UA. Then the transition graph is transformed to the form of Figure 2.

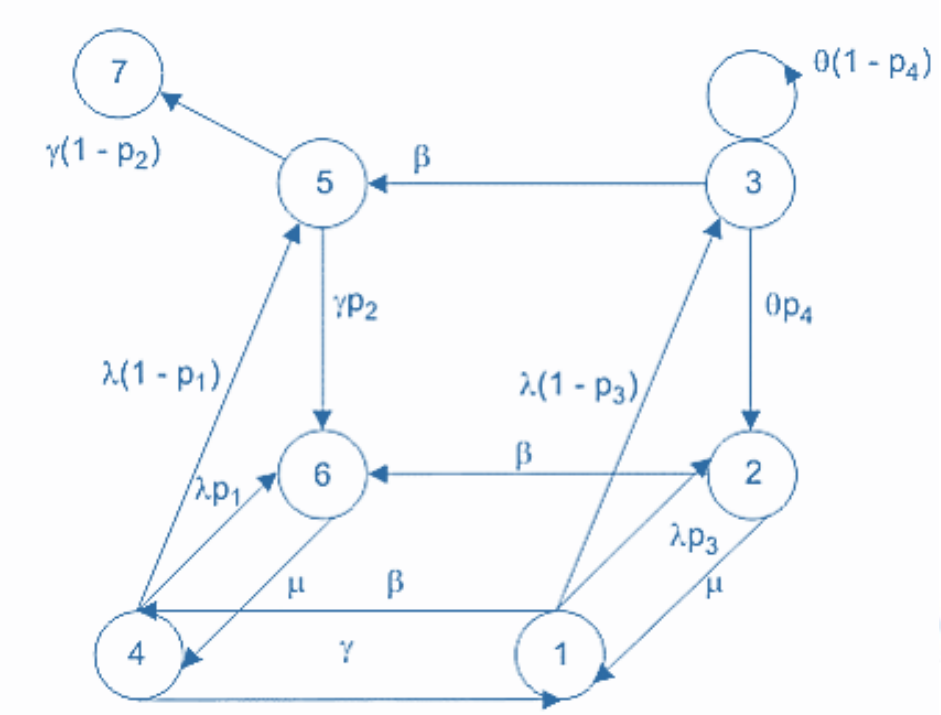

Fig. 2. Graph of transitions of the process under research with an absorbing state

This graph corresponds to the transition matrix and the vector of the average residence time in each of the marked states:

$$\hat{P} = \begin{matrix} 0 & \frac{p_3\lambda}{\beta+\lambda} & \frac{(1-p_3)\lambda}{\beta+\lambda} & \frac{\beta}{\beta+\lambda} & 0 & 0 & 0 \\ \frac{\mu}{\beta+\mu} & 0 & 0 & 0 & 0 & \frac{\beta}{\beta+\mu} & 0 \\ 0 & \frac{p_4\theta}{\beta+\theta} & \frac{(1-p_4)\theta}{\beta+\theta} & 0 & \frac{\beta}{\beta+\theta} & 0 & 0 \\ \frac{\gamma}{\lambda+\gamma} & 0 & 0 & 0 & \frac{(1-p_1)\lambda}{\lambda+\gamma} & \frac{p_1}{\lambda+\gamma} & 0 \\ 0 & 0 & 0 & 0 & 0 & p_2 & 1-p_2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

$$\|m_i\| = \frac{1}{\beta+\lambda} \quad \frac{1}{\beta+\mu} \quad \frac{1}{\beta+\theta} \quad \frac{1}{\lambda+\gamma} \quad \frac{1}{\gamma} \quad \frac{1}{\mu} \quad \infty .$$

Since the system under consideration is characterized by the presence of an absorbing state S7, the mathematical expression for the average operating time of a technical means of protecting information from unauthorized access can be defined as the average time spent by the considered process in the set of non-returning states (S1 - S6).

Conclusion

Research work is important due to the development of information technologies and the relevance of information security issues. In the study, the issue of unauthorized access to information from the point of view of reliability theory is based on a fundamental and practical basis. It served to show the processes in the researched system with the help of graphs, to increase the accuracy of the research work. It is also possible to continue this work as a method in various information security systems.

References

1. A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.
2. I. Yarashov, "Algorithmic Formalization Of User Access To The Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-3, doi: 10.1109/ICISCT52966.2021.9670023.
3. A. Kabulov, I. Normatov, I. Kalandarov and I. Yarashov, "Development of An Algorithmic Model And Methods For Managing Production Systems Based On Algebra Over Functioning Tables," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670307.
4. A. Kabulov, I. Saymanov, I. Yarashov and A. Karimov, "Using Algorithmic Modeling to Control User Access Based on Functioning Table," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850.
5. A. Kabulov, I. Kalandarov and I. Yarashov, "Problems Of Algorithmization Of Control Of Complex Systems Based On Functioning Tables In Dynamic Control Systems," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670017.
6. A. Kabulov and I. Yarashov, "Mathematical model of Information Processing in the Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670192.
7. A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.
8. Kabulov A. V., Yarashov I. K., Jo‘Rayev M. T. Computer viruses and virus protection problems //Science and Education. – 2020. – Т. 1. – №. 9. – С. 179-184.
9. Kabulov A. et al. Algorithmic method of security of the Internet of Things based on steganographic coding. 2021 IEEE International IOT //Electronics and Mechatronics Conference, IEMTRONICS. – 2021.
10. Madrahimova D., Yarashov I. Limited in solving problems of computational mathematics the use of elements //Science and Education. – 2020. – Т. 1. – №. 6. – С. 7-14.
11. Kabulov A., Yarashov I., Vasiyeva D. SECURITY THREATS AND CHALLENGES IN IOT TECHNOLOGIES //Science and Education. – 2021. – Т. 2. – №. 1. – С. 170-178.

12. Kabulov A., Muhammadiyev F., Yarashov I. ANALYSIS OF INFORMATION SYSTEM THREATS //Science and Education. – 2020. – Т. 1. – №. 8. – С. 86-91.
13. Gaynazarov S. M. et al. ALGORITHM OF MOBILE APPLICATION FOR MEDICINE SEARCH //Science and Education. – 2020. – Т. 1. – №. 8. – С. 600-605.
14. Кабулов А. В. Шерзод Туйлибоевич Болтаев, and Гулдофарид Муроджоновна Хабибжонова.«АЛГОРИТМИЧЕСКИЕ АВТОМАТНЫЕ МОДЕЛИ И МЕТОДЫ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ МИКРОПРОЦЕССОРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.» //WORLD SCIENCE: PROBLEMS AND INNOVATIONS. – 2019.
15. Yarashov I., Normatov I., Mamatov A. THE STRUCTURE OF THE ECOLOGICAL INFORMATION PROCESSING DATABASE AND ITS ORGANIZATION //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 114-117.
16. Yarashov I., Normatov I., Mamatov A. ECOLOGICAL INFORMATION PROCESSING TECHNOLOGIES AND INFORMATION SECURITY //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 73-76.
17. Kabulov A., Yarashov I., Mirzataev S. DEVELOPMENT OF THE IMPLEMENTATION OF IOT MONITORING SYSTEM BASED ON NODE-RED TECHNOLOGY //Karakalpak Scientific Journal. – 2022. – Т. 5. – №. 2. – С. 55-64.
18. I. Yarashov, "Development of a reliable method for grouping users in user access control based on a Functioning table," 2022 International Conference on Information Science and Communications Technologies (ICISCT), 2022, pp. 1-5.
19. Normatov I., Yarashov I., Boboqulov B. Development of models for describing the processing of environmental information in security problems of controlling a protection system based on petri nets //Central Asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 229-239.
20. Kabulov A., Yarashov I., Daniyarov B. Systematic analysis of blockchain data storage and sharing technology //Central Asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 240-247.
21. Jumaboyeva A., Yarashov I. Maxsus maktabgacha ta’lim tashkilotlarida nutqida nuqsoni bo‘lgan bolalarni axborot texnologiyalari asosida pedagogik metodlar orqali tahlil qilish// O'zbekistonda ilmiy - amaliy tadqiqotlar mavzusida Respublika 17-ko'p tarmoqli ilmiy masofaviy onlayn konferentsiya.-2020.-C.249-250.
22. Kabulov A.V., **Yarashov I.K.** Algorithmic model of synthesis and elimination of risks based on Functioning table. Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.205-206.
23. Kabulov A.V., **Yarashov I.K.** Algorithmic modeling user access control based on Functioning table. Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.206-207.
24. Kabulov A.V., **Yarashov I.K.,** Kalandarov I.I., Otakhonov A.A. Algorithmic analysis of a system based on a Functioning table and importance for information security. Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.207-208.
25. Yarashov I, Normurodov D. “Parol bo‘yicha autentifikasiyalashning asosiy tahdidlari va shaxsiy parolning zaiflik”. Uzliksiz ma'naviy tarbiya kontsepsiyasini amalga oshirishdagi ommaviy axborot vositalarining roli mavzusida Respublika onlayn ilmiy-amaliy konferentsiya, 2020.pp 492-496.

26. Islambek Saymanov, Inomjon Yarashov. “IoT arxitekturasida funksional darajalari tahlili”. Ijtimoiy sohalarni raqamlashtirishda innovasion texnologiyalarning o'rni va ahamiyati Respublika ilmiy-amaliy konferensiya. 2020. Karshi, pp 359-361.
27. Inomjon Yarashov, Normatov Dilmurod. “Kiber fizik tizimlar va Iot tizimlarning qiyosiy tahlili”. Axborot-kommunikasiya texnologiyalari va telekommunikasiyalarning zamonaviy muammolari va yechimlari Respublika ilmiy-texnik konferensiya, 2020 . Fergana, pp 338-340.